IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

DAVID SMITH, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

COMMUNITY HEALTH SYSTEMS, INC. and COMMUNITY HEALTH SYSTEMS PROFESSIONAL SERVICES CORPORATION,

Defendants.

Civil Action No.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

NOW COMES Plaintiff, David Smith ("Plaintiff"), by and through his undersigned counsel, individually and on behalf of all others similarly situated, and hereby files this Class Action Complaint against Community Health Systems, Inc. ("CHS") and Community Health Systems Professional Services Corporation ("CHSPSC") (collectively "Defendants"). In support thereof, Plaintiff states and alleges as follows:

NATURE OF THE ACTION

1. Plaintiff brings this nationwide Class Action Complaint on behalf of himself and all other individuals whose patient identification data was stolen from the computer network of Defendants (the "Data Breach").

2. As a result of Defendants' failure to protect this highly sensitive and confidential information, the patient identification data of Plaintiff and the members of the proposed Class, including but not limited to patient names, addresses, birthdates, telephone numbers and Social Security numbers, was obtained by unknown third parties.

3. Defendants had a duty to protect the private, highly sensitive, confidential patient identification data of Plaintiff and the members of the proposed Class.

4. Defendants agreed to protect the private, highly sensitive, confidential patient identification data of Plaintiff and the members of the proposed Class.

5. Defendants failed to safeguard and prevent vulnerabilities from being taken advantage of in their computer system.

6. Intruders first gained access to Defendants' computer network in April, 2014. However, Defendants did not confirm the Data Breach until July, 2014. Defendants then waited until August, 2014 to begin sending out notifications about the Data Breach.

7. Plaintiff and the proposed Class members have a possessory interest in their patient identification data and an interest in it remaining private because that information, including incredibly private and sensitive information such as Social Security numbers, has substantial value not only to Plaintiff and the proposed Class members, but to also criminals who traffic in such information.

8. Because of the real threat of immediate harm, as well as the intrinsic value of the stolen information itself, Plaintiff and the proposed Class members have suffered an immediate and present injury to their privacy and possessory interest as a direct result of Defendants' negligent failure to safeguard Plaintiff's and the proposed Class members' confidential patient identification data, as well as the breach of their agreements to do the same.

9. Moreover, Plaintiff and the proposed Class members are at an increased and imminent risk of becoming victims of identity theft crimes, fraud and abuse, and have been forced to spend considerable time and money to protect themselves as a result of Defendants' conduct.

THE PARTIES

10. Defendant Community Health Systems, Inc. is one of the nation's leading operators of general acute care hospitals. The organization's affiliates own, operate, or lease 206 hospitals in 29 states with approximately 31,100 licensed beds.

11. Defendant Community Health Systems, Inc. is headquartered at 4000 Meridian Boulevard, Franklin, Tennessee 37067.

12. Defendant Community Health Systems Professional Services Corporation provides management, consulting, and information technology services to independent community hospitals and health systems, as well as to certain clinics and physician practice operations.

13. Defendant Community Health Systems Professional Services Corporation operates as a subsidiary of Defendant Community Health Systems, Inc.

14. Defendant Community Health Systems Professional Services Corporation is headquartered at 4000 Meridian Boulevard, Franklin, Tennessee 37067.

15. Within the last five (5) years, Plaintiff has been treated by Defendants' subsidiary health care provider, Sharon Regional Health System located in Sharon, Pennsylvania.

JURISDICTION AND VENUE

16. This Court has original jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2). The amount in controversy in this action exceeds $5,000,000, exclusive of interest and costs, and there are more than 100 members of the Class defined below, the majority of whom reside in different states than Defendants.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391, because Defendants regularly transact business in this District, and a substantial part of the events giving rise to this

Complaint arose in this District.

FACTUAL BACKGROUND

18. Plaintiff and the proposed Class members were required to provide their health care providers with highly sensitive, private, and confidential patient identification data, including their full legal names, addresses, birthdates, telephone numbers and Social Security numbers in order to receive the healthcare they required.

19. Through their subsidiary and other relationships with Plaintiff and the proposed Class members' health care providers, Defendants came into possession of the patient identification data of Plaintiff and the proposed Class members.

20. The patient identification data of Plaintiff and the proposed Class members, while under the control of Defendants, was accessed without the authorization of Plaintiff and the proposed Class members.

21. Although intruders first gained access to Defendants' computer network in April 2014, Defendants did not confirm the Data Breach until July 2014.

22. Defendants then waited until August 2014 to begin sending out notifications about the Data Breach.

23. On August 18, 2014, Defendants filed a Form 8-K with the United States Securities and Exchange Commission ("SEC") that provided the first notification of the Data Breach. The filing stated:

> In July 2014, Community Health Systems, Inc. (the "Company") confirmed that its computer network was the target of an external, criminal cyber-attack that the Company believes occurred in April and June, 2014. The Company and its forensic expert, Mandiant (a FireEye Company), believe the attacker was an "Advanced Persistent Threat" group originating from China who used highly sophisticated malware and technology to attack the Company's systems. The attacker was able to bypass the Company's security measures and successfully copy and transfer certain data outside the Company. Since first learning of this

> attack, the Company has worked closely with federal law enforcement authorities in connection with their investigation and possible prosecution of those determined to be responsible for this attack. The Company also engaged Mandiant, who has conducted a thorough investigation of this incident and is advising the Company regarding remediation efforts. Immediately prior to the filing of this Report, the Company completed eradication of the malware from its systems and finalized the implementation of other remediation efforts that are designed to protect against future intrusions of this type. The Company has been informed by federal authorities and Mandiant that this intruder has typically sought valuable intellectual property, such as medical device and equipment development data. However, in this instance the data transferred was non-medical patient identification data related to the Company's physician practice operations and affected approximately 4.5 million individuals who, in the last five years, were referred for or received services from physicians affiliated with the Company. The Company has confirmed that this data did not include patient credit card, medical or clinical information; the data is, however, considered protected under the Health Insurance Portability and Accountability Act ("HIPAA") because it includes patient names, addresses, birthdates, telephone numbers and social security numbers. The Company is providing appropriate notification to affected patients and regulatory agencies as required by federal and state law. The Company will also be offering identity theft protection services to individuals affected by this attack. The Company carries cyber/privacy liability insurance to protect it against certain losses related to matters of this nature. While this matter may result in remediation expenses, regulatory inquiries, litigation and other liabilities, at this time, the Company does not believe this incident will have a material adverse effect on its business or financial results.

24. On August 19, 2014, Defendants published a "Data Breach Notification" on their public website. The Notification stated:

> On behalf of Community Health Systems Professional Services Corporation ("CHSPSC"), I want to express sincere regret to the patients of affiliated physician practices and clinics whose data was accessed in a foreign-based cyber-attack of our computer network. We value the trust you have placed in us for your care and it is our priority to ensure those who were affected by this attack are notified about the breach and have their questions answered. If you were affected by the data breach, you will receive a letter with more information and a toll-free number to call to learn about the free identity theft protection offered to affected patients. The following notice contains more details about the breach, measures we are taking to notify you, and how we are improving the way we protect health your information.
>
> In July 2014, Community Health Systems Professional Services Corporation ("CHSPSC") confirmed its computer network was the target of an external criminal cyber-attack in April and June 2014. CHSPSC, a Tennessee company,

> provides management, consulting, and information technology services to certain clinics and hospital-based physicians in this area.
>
> CHSPSC believes the attacker was an "Advanced Persistent Threat" group originating from China, which used highly sophisticated malware technology to attack CHSPSC's systems. The intruder was able to bypass the company's security measures and successfully copy and transfer some data existing on CHSPSC's systems.
>
> Since first discovering the attack, CHSPSC has worked closely with federal law enforcement authorities in connection with their investigation of the matter. CHSPSC also engaged an outside forensic expert to conduct a thorough investigation and remediation of this incident. CHSPSC has implemented efforts designed to protect against future intrusions. These efforts include implementing additional audit and surveillance technology to detect unauthorized intrusions, adopting advanced encryption technologies, and requiring users to change their access passwords.
>
> The majority of patients of clinics and hospital-based physicians affiliated with CHSPSC were not affected by this breach. Individuals whose information was taken in this cyber-attack will be mailed a letter informing them about the data breach and how to enroll in free identity theft protection and credit monitoring services. The data taken includes patients' names, addresses, birthdates, social security numbers, and, in some cases, telephone numbers, and the names of employers or guarantors. However, to the best of CHSPSC's knowledge, NO credit card information was taken and NO medical or clinical information was taken. CHSPSC recommends that you remain vigilant for incidents of fraud and identity theft by reviewing your credit report and accounts for unauthorized activity.
>
> Anyone with questions or concerns about this cyber-attack may contact 1-855-205-6951 toll-free beginning Wednesday, August 20, 2014, at 8:00 a.m. central time. For information on preventing identity theft or to report suspicious activity, contact the Federal Trade Commission at 1-877-438-4338 or get free information at www.ftc.gov.[1]

25. Defendants did not send Plaintiff correspondence notifying him of the Data Breach until several weeks following said breach.

26. Defendants' failure to notify Plaintiff and proposed Class members of the Data Breach in a reasonable time deprived Plaintiff and proposed Class members of critical time to

[1] Defendants' August 19, 2014, Data Breach Notification is available at http://www.chs.net/media-notice-august-19-2014/.

protect themselves from identity theft.

27. Nationally, approximately four and one-half (4.5) million individuals have had their patient identification data misappropriated as a result of the breach of Defendants' computer network.

28. Defendants had a duty to protect the private, highly sensitive, confidential patient identification data of Plaintiff and the proposed Class members.

29. The patient identification data that was copied and transferred from Defendants' computer systems is considered protected under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 29 U.S.C.A. §§ 1181 *et seq.* because it includes patient names, addresses, birthdates, telephone numbers and Social Security numbers.

30. HIPAA required Defendants to "reasonably protect" the copied data from "any intentional or unintentional use or disclosure." 45 C.F.R. § 164.530(c)(1)(2)(i). Federal regulations also required Defendants to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." *Id.* at § 164.530(c)(1).

31. Defendants violated HIPAA by failing to maintain the confidentiality of Plaintiff's and the proposed Class members' protected patient identification data.

32. Defendants failed to safeguard and prevent vulnerabilities from being taken advantage of in their computer systems.

33. As a result of Defendants' failure to safeguard and prevent vulnerabilities from being taken advantage of in their computer systems, unauthorized third parties were able to bypass Defendants' inadequate security measures and successfully copy and transfer the patient identification data of Plaintiff and the proposed Class members.

34. The 2013 Identity Fraud Report released by Javelin Strategy & Research reports that in 2012 identity fraud incidents increased by more than one million victims and fraudsters stole nearly $21 billion. The study found 12.6 million victims of identity fraud in the United States in the past year, which equates to 1 victim every 3 seconds. The report also found that nearly 1 in 4 data breach letter recipients became a victim of identity fraud, with breaches involving Social Security numbers to be the most damaging.

35. To assist companies in protecting the security of sensitive personal and financial information, the Federal Trade Commission ("FTC") has issued a publication entitled "Protecting Personal Information: A Guide for Business" (the "FTC Report"). In this publication, the FTC provides guidelines for businesses on how to develop a "sound data security plan" to protect against crimes of identity theft.

36. To protect the personal sensitive information in their files, the FTC Report instructs businesses to follow the following guidelines:

a) Keep inventory of all computers and laptops where the company stores sensitive data;

b) Do not collect personal information if there is no legitimate business need. If there is a legitimate business need, only keep the information as long as necessary;

c) Use Social Security numbers only for required and lawful purposes and do not store these numbers unnecessarily, such as for an employee or customer identification number;

d) Encrypt the personal information, particularly if the sensitive information is shipped to outside carriers or contractors. In addition, the business should keep

an inventory of all the information it ships;

e) Do not store sensitive computer data on any computer with an Internet connection or access unless it is essential for conducting the business;

f) Control access to sensitive information by requiring that employees use "strong" passwords; and

g) Implement information disposal practices that are reasonable and appropriate to prevent unauthorized access to personally identifying information.

37. Defendants violated federal guidelines and failed to meet current data security industry standards by failing to ensure adequate security over Plaintiff's and the proposed Class members' patient identification data and by failing to retain Plaintiff's and the proposed Class members' patient identification data in a secure and safe manner.

38. By way of illustration and without limitation, on information and belief, Defendants failed to properly encrypt data, failed to establish adequate firewalls to handle a server intrusion contingency, and failed to implement adequate authentication protocol to protect the confidential information contained in its computer network.

39. On information and belief, the Data Breach also resulted from Defendants' pattern of un-patched systems and inadequate vulnerability management.

40. Plaintiff and the proposed Class members and Defendants agreed that, as part of the health care services provided to Plaintiff and the proposed Class Members, Defendants would protect the patient identification data of Plaintiff and the proposed Class members.

41. Specifically, Defendants have published a "Code of Conduct," available at http://www.chs.net/wp-content/uploads/PDF/2014%20Code%20of%20Conduct.pdf (last visited Nov. 20, 2014).

42. Defendants' Code of Conduct contains at "Statement of Beliefs" which provides, in relevant part, as follows: "We have adopted the following Statement of Beliefs that summarizes the commitments of the organization's constituents ***to our patients***, colleagues, physicians, and the communities served. … [W]e are dedicated to compliance with all federal, state, and local laws, rules, and regulations, ***including privacy and security of patient health information***." *See* Defendants' Code of Conduct at 2 (emphasis added).

43. Further, the provisions of Defendants' Code of Conduct concerning the "Confidentiality of Patient Information" provide that:

> ***When a patient enters a CHS affiliated facility, a large amount of personal, medical, and insurance data is collected and used to satisfy information needs including the ability to make decisions about a patient's care. We consider patient information highly confidential.*** Colleagues are expected to take care to protect the privacy of individually identifiable health information at all times. All of the facilities within the organization have specific policies describing patient confidentiality and release of information rules that conform to federal, state, and local laws governing the release or disclosure of health information.

See Defendants' Code of Conduct at 10 (emphasis added).

44. Moreover, Defendants' health care providers have published patient resources regarding "Patient Rights & Responsibilities" and "HIPAA Compliance." By way of example, on its public website, Brandywine Hospital, which is owned and operated by Defendants, assures patients, such as Plaintiff and members of the proposed Class, that they have the right to "[p]ersonal privacy" and "privacy of your health information." *See* http://www.brandywine hospital.com/brandywine-hospital/patientrightsandresponsibilities.aspx.

45. Brandywine Hospital further assures patients, such as Plaintiff and members of the proposed Class, of its "Pledge Regarding Medical Information," stating that "[w]e understand that medical information about you and your health care is personal. We are committed to protecting medical information about you." *See* http://www.brandywinehospital.com

/brandywine-hospital/hipaa1.aspx.

46. These agreements to protect Plaintiff's and the proposed Class members' patient identification data were a value added to the services provided by Defendants' health care providers that were considered a benefit of the bargain for which Plaintiff and the proposed Class members paid adequate consideration.

47. A portion of the consideration paid for healthcare (treatment?) by Plaintiff and the proposed Class members was accepted by Defendants and was allocated to protecting and securing Plaintiff's and the proposed Class members' patient identification data and ensuring HIPAA compliance. This allocation was made for the purpose of offering patients and consumers, such as Plaintiff and the proposed Class members, added value to the health care services provided by agreeing to protect their patient identification data.

48. As a direct result of Defendant's negligent failure to maintain reasonable and adequate security procedures to protect against the theft of Plaintiff's and the proposed Class members' patient identification data, and Defendants' breach of their agreements to do so, Plaintiff and the proposed Class members are at an increased and imminent risk of becoming victims of identity theft crimes, fraud and abuse.

49. In addition, Plaintiff and the proposed Class members have spent, and will need to spend, considerable time and money to protect themselves as a result of Defendants' conduct.

CLASS ACTION ALLEGATIONS

50. Plaintiff brings this action as a Class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on his own behalf and on behalf of all similarly situated persons,

defined as follows:

> All persons in the United States whose patient identification data was contained in or on Defendants' computer network, whose patient identification data was misappropriated as a result of the Data Breach.

51. Plaintiff is a member of the Class he seeks to represent.

52. The Class is so numerous that joinder of all members is impracticable, as approximately four and one-half (4.5) million individuals' patient identification data has been compromised.

53. The members of the Class are individuals who were referred for or received services from physicians affiliated with Defendants. As such, the members of the Class are readily ascertainable, as they can be identified by records maintained by Defendants. Notice can be provided by means permissible under Rule 23.

54. Plaintiff's claims are typical of the claims of all members of the Class. Specifically, Plaintiff's and Class members' claims arise from Defendants' failure to install and maintain reasonable security measures, and to implement appropriate policies, to protect Plaintiff's and Class members' patient identification data.

55. The conduct of Defendants has caused injury and/or imminent threat of injury to Plaintiff and members of the Class.

56. Prosecuting separate actions by individual Class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards of conduct for Defendants.

57. Plaintiff will fairly and adequately represent the interests of the Class. Plaintiff has no interests antagonistic to or in conflict with those of the proposed Class members and therefore is an adequate representative for the proposed Class members.

58. Plaintiff is represented by experienced counsel who are qualified to litigate this case.

59. Common questions of law and fact predominate over individualized questions. A Class action is superior to all other available methods for the fair and efficient adjudication of this controversy.

60. There are questions of law and fact common to all members of the Class, the answers to which will advance the resolution of the claims of the Class members and that include, without limitation:

a) Whether Defendants failed to provide adequate security and/or protection for their computer systems containing Plaintiff's and the proposed Class members' patient identification data;

b) Whether Defendants owed a legal duty to Plaintiff and the proposed Class members to protect their personal and financial information and whether Defendants breached this duty;

c) Whether the conduct of Defendants resulted in the unauthorized breach of their computer systems containing Plaintiff's and the proposed Class members' patient identification data;

d) Whether Plaintiff and the proposed Class members have been injured by Defendants' conduct;

e) Whether Plaintiff and Class members are at an increased risk of identity theft as a result of Defendants' failure to protect Plaintiff's and the proposed Class members' patient identification data;

f) Whether Defendants were negligent;

g) Whether Defendants are in breach of contract;

h) Whether Plaintiff and the proposed Class members are entitled to injunctive relief; and

i) Whether Plaintiff and the proposed Class members are entitled to damages, and the measure of such damages.

COUNT I
NEGLIGENCE

61. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

62. Defendants had a duty to exercise reasonable care to protect and secure Plaintiff's and the proposed Class members' patient identification data within its possession or control from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This highly confidential patient identification data includes but is not limited to patient names, addresses, birthdates, telephone numbers, Social Security numbers, and other personal information.

63. Defendants' duty included, among other things, designing, maintaining, and testing their security systems to ensure that Plaintiff's and the proposed Class members' patient identification data in their possession was adequately secured and protected.

64. Defendants further had a duty to implement processes that would detect a breach of their security systems in a timely manner.

65. Through their acts or omissions, Defendants breached their duty to use reasonable care to protect and secure Plaintiff's and the proposed Class members' patient identification data within their possession or control. Defendants breached their duty by failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and

proposed Class members' patient identification data, failing to adequately monitor the security of their networks, allowing unauthorized access to Plaintiff's and the proposed Class members' patient identification data, and failing to recognize in a timely manner that Plaintiff's and proposed Class members' patient identification data had been compromised.

66. Defendants' failure to comply with widespread industry standards relating to data security, as well as the delay between the date of the intrusion and the date Plaintiff and proposed Class members were informed of the Data Breach, further evince Defendants' negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and the proposed Class members' patient identification data in their possession or control.

67. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and the proposed Class members, the Data Breach would not have occurred and Plaintiff's and the proposed Class members' patient identification data would not have been compromised.

68. The injury and harm suffered by Plaintiff and the proposed Class members was the reasonably foreseeable result of Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the proposed Class members' patient identification data in their possession or control. Defendants knew or should have known that their systems and technologies for processing and securing Plaintiff's and proposed Class members' patient identification data had security vulnerabilities.

69. Plaintiff is part of a well-defined foreseeable Class. Defendants' liability is restricted to a finite and discernable Class who were well-known and identifiable to Defendants before their conduct caused the harm at issue. Members of the Class are persons who utilized services from Defendants' health care providers, meaning that the persons comprising the Class,

their numbers, and their potential to be harmed by Defendants' negligent conduct all were predictable and reasonably foreseeable.

70. The nature of the harm was also foreseeable. Defendants were aware, or should have been aware, that the patient identification data provided by Plaintiff and Class members was frequently the target of data breach crimes because that information was utilized to engage in identity theft. Being aware of both the potential for attempted theft and the discernible class of persons who entrusted Defendants with their valuable patient identification data, Defendants had a duty to ensure that they protected that information.

71. Defendants' negligent handling of Plaintiff's sensitive information was the direct and proximate cause of her foreseeable economic harm. Upon acquisition, Defendants had sole control over the data and Plaintiff had no ability to protect her information. Consequently, Defendants were in the best and only position to safeguard the information. Defendants failed in this regard and negligently allowed third party hackers to access their servers and remove (copy?) Plaintiff's information. Thus, Defendants' negligence directly made available Plaintiff's personal information and therefore was a direct cause of Plaintiff's and all proposed Class members' harm.

72. As a result of Defendants' negligence, Plaintiff and the proposed Class members have suffered actual damages including but not limited to expenses for credit monitoring, lost work time, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

73. As a result of Defendants' negligence, Plaintiff and the proposed Class members are at an increased and imminent risk of becoming victims of identity theft crimes, fraud and abuse.

COUNT II
BREACH OF CONTRACT

74. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

75. Defendants came into possession of Plaintiff's and the proposed Class members' patient identification data through their subsidiary and other relationships with the health care providers of Plaintiff and the proposed Class members.

76. Defendants contracted with Plaintiff and the proposed Class members to protect such information.

77. The written agreement between Defendants and Plaintiff and the proposed Class members expressly required Defendants to safeguard and protect Plaintiff's and the proposed Class members' patient identification data from being compromised and/or stolen. In the agreement the Defendants also promised to comply with HIPAA and its implementing regulations and only to disclose Plaintiff's and the proposed Class members' patient identification information when required to do so by federal and/or state law.

78. Plaintiff and the proposed Class members were direct beneficiaries of the contract between themselves and Defendants, and Defendants owed a direct duty of care to them.

79. To the extent that an express contract was not created by the written agreement, an implied contract was created when Plaintiff and the proposed Class members disclosed their patient identification data to Defendants in exchange for healthcare, for which Plaintiff and the proposed Class members then paid.

80. Plaintiff and the proposed members of the Class would not have disclosed such information without assurance that Defendants would maintain sufficient security measure to prevent its unauthorized access, theft, or otherwise improper disclosure.

81. Plaintiff and the proposed members of the Class also disclosed such information for the benefit of Defendants.

82. Thus, the provision of the patient identification information by Plaintiff and the proposed members of the Class and Defendants acceptance, created an implied contract whereby Defendant had a duty to safeguard and protect the information of Plaintiff and the proposed members of the Class.

83. Defendants did not safeguard or protect Plaintiff's and the proposed Class members' personal identification data from being accessed, compromised, and/or stolen. Defendants did not maintain sufficient security measures and procedures to prevent unauthorized access to Plaintiff's and the proposed Class members' patient identification data.

84. Because Defendants failed to safeguard and/or protect Plaintiff's and the proposed Class members' patient identification data from being compromised or stolen, Defendants breached their contracts with Plaintiff and the proposed Class members.

85. Plaintiff and the proposed Class members have suffered and will continue to suffer damages as the result of Defendants' breach.

COUNT III
NEGLIGENCE PER SE

86. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

87. HIPAA was designed to protect the privacy of personal medical information by limiting is disclosure.

88. HIPAA seeks to protect the privacy of protected patient identification data by prohibiting any voluntary or involuntary use or disclosure of such data in violation of the directives set out in the statute and its regulations.

89. As described above, Defendants violated HIPAA by failing to maintain the confidentiality of their protected patient identification data.

90. Plaintiff and the proposed Class members have suffered harm, including but not limited to expenses for credit monitoring, lost work time, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm, as well as an being placed at an increased and imminent risk of becoming victims of identity theft crimes, fraud and abuse as a result of Defendants' violation.

91. Plaintiff and the proposed Class members are persons whom Congress intended to be protected by HIPAA.

92. Defendant is a HIPAA covered entity.

93. The records stolen from Plaintiff and other Class members are the types of records HIPAA was created to protect.

94. The injuries suffered by Plaintiff and the proposed Class members were directly and proximately caused by Defendants' violation of HIPAA.

95. Defendants' violation of HIPAA thus constitutes negligence per se and Plaintiff and the proposed Class members are entitled to recover damages in an amount to be proven at trial.

COUNT IV
BAILMENT

96. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

97. Plaintiff and the proposed Class members delivered their patient identification data to Defendants in order to receive health care services from Defendants' affiliated health care providers.

98. This patient identification data was furnished to Defendants for the exclusive purpose of administering and managing health care services delivered by Defendants' affiliated health care providers and Defendants took possession of the patient identification data for the same reason.

99. Upon delivery, Plaintiff and the proposed Class members intended and understood that Defendants would adequately safeguard their patient identification data and Defendants, in accepted possession, understood the expectations of Plaintiff and the proposed Class members. Accordingly, bailment was established for the mutual benefit of the parties at the time of delivery and acceptance of possession.

100. Pursuant to the bailment arrangement, Defendants owed Plaintiff and the proposed Class members a duty of reasonable care in safeguarding and protecting their patient identification data.

101. This duty was breached by Defendants' failure to take adequate steps to cure the deficiencies in their security protocols and Defendants' failure to conform to best practices and industry standards to prevent unauthorized access to Plaintiff's and the proposed Class members' patient identification data.

102. As a direct proximate result of Defendants' breach, the patient identification data of Plaintiff and the proposed Class members was exposed to third parties and thereafter stolen, resulting in damage to the personal identities of Plaintiff and the proposed Class members.

COUNT V
UNJUST ENRICHMENT

103. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

104. Plaintiff brings this Count V in the alternative to her claim for breach of

contract.

105. Defendants received payment from Plaintiff and the proposed Class members to perform services that included protecting Plaintiff's and the proposed Class members' patient identification data.

106. Defendants did not protect Plaintiff's and the proposed Class members' patient identification data, but retained Plaintiff's and the proposed Class members' payments.

107. Defendants retained the benefits of Plaintiff's and the proposed Class members' payments under circumstances which rendered it inequitable and unjust for Defendants to retain such benefits without paying for their value.

108. Defendants have knowledge of said benefits.

109. As a result, Plaintiff and the proposed Class members have been proximately harmed and/or injured.

COUNT VI
WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT

110. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

111. The Fair Credit Reporting Act ("FCRA") "require[s] consumer reporting agencies [to] adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information." 15 U.S.C. § 1681(b).

112. The FCRA protects the disclosure of medical information and only allows dissemination in a limited number of circumstances. *See* 15 U.S.C. §1681a(d)(3); § 1681b(g); § 1681(a)(6).

113. Plaintiff's and the proposed Class members' patient identification data constitutes "medical information" for purposes of the FCRA.

114. Defendants are "consumer reporting agencies" because "for monetary fees, dues, [and/]or on a cooperative nonprofit basis, [they] regularly engage[] in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and [] use . . . interstate commerce for the purpose of preparing or furnishing consumer reports." 15 U.S.C. § 1681a(f).

115. Defendants' collection of Plaintiff's and the proposed Class member's patient identification data and subsequent transmission and communication of the same constitutes as a "consumer report" because the information collected "bear[s] on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" and "is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes." 15 U.S.C. § 1681a(d)(1).

116. Defendants, as consumer reporting agencies, were required (and still are required) to put in place and maintain procedures that would protect the patient identification data of Plaintiff and the proposed members of the Class and limit its disclosure exclusively to those situations outlined in the FCRA. Defendants failed to put in place and/or maintain the requisite procedures and thereby caused Plaintiff's and the proposed Class members' information to be disclosed in violation of the FCRA, directly resulting in the theft and wrongful dissemination of that information.

117. Defendants' violation was willful and/or reckless and has directly caused (and

continues to cause) damage to Plaintiff and the Class including cost of credit monitoring and identity-theft insurance, other out-of pocket expenses, identity theft, loss of privacy, and other economic and non-economic damages.

118. Thus, Plaintiff and the Class are entitled to statutory damages, non-statutory damages in an amount to be proven at trial, and attorneys' fees.

COUNT VII
NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT

119. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

120. In the alternative, Defendants negligently violated the FCRA by failing to put in place and maintain procedures designed to protect Plaintiff's and the proposed Class members' patient identification data and limit its disclosure solely to the situations outlined in the FCRA.

121. As described above, this failure proximately caused the theft and wrongful dissemination of the protected patient identification information.

122. It was reasonably foreseeable that Defendants failure to put in place and maintain procedures to protect and limit the disclosure of Plaintiff's and the proposed Class members' patient identification data would result in the theft, unlawful dissemination and/or wrongful disclosure of the data.

123. Defendants' violation was negligent and has directly caused (and continues to cause) damage to Plaintiff and the Class including cost of credit monitoring and identity-theft insurance, other out-of pocket expenses, identity theft, loss of privacy, and other economic and non-economic damages.

124. Thus, Plaintiff and the Class are entitled to statutory damages, non-statutory damages in an amount to be proven at trial and attorneys fees.

PRAYER FOR RELIEF

125. Plaintiff requests that this Court enter judgment against Defendants and in favor of Plaintiff and the proposed Class members and award the following relief:

a) That this action be certified as a Class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, declaring Plaintiff as the representative of the Class and Plaintiff's counsel as counsel for the Class;

b) Monetary damages;

c) Injunctive relief, including but not limited to the provision of credit monitoring services for Plaintiff and the proposed Class members for a period of at least twenty-five (25) years, the provision of bank monitoring services for Plaintiff and the proposed Class members for a period of at least twenty-five (25) years, the provision of credit restoration services for Plaintiff and the proposed Class members for a period of at least twenty- five (25) years, and the provision of identity theft insurance for Plaintiff and the proposed Class members for a period of at least twenty-five (25) years;

d) Reasonable attorneys' fees and expenses, including those related to experts and consultants;

e) Costs;

f) Pre and post judgment interest;

g) Such other relief as this Court may deem just and proper.

JURY DEMAND

126. Pursuant to Fed. R. Civ. P. 38(b), Plaintiff, individually and on behalf of the Class he seeks to represent, demands a trial by jury for all issues so triable.

Respectfully submitted,

Dated: MARCH 24, 2015

By: /s/ D. Aaron Rihn

D. AARON RIHN, ESQUIRE
Pa. I.D. No.: 85752
ROBERT PEIRCE & ASSOCIATES, P.C.
Firm I.D. No.: 839
2500 Gulf Tower, 707 Grant Street
Pittsburgh, PA 15219
Telephone: (412) 281-7229
Emails: arihn@peircelaw.com

/s/ Jason A. Medure

JASON A. MEDURE, ESQUIRE
Pa. I.D. No.: 90976
MEDURE, BONNER, BELLISSIMO, PEIRCE & DALEY, LLC
22 North Mill Street
New Castle, PA 16101
Telephone: (724) 653-7855
Emails: jmedure@medurelaw.com